25X1

OPENING REMARKS

WILLIAM J. CASEY, DIRECTOR OF CENTRAL INTELLIGENCE

SENATE SELECT COMMITTEE ON INTELLIGENCE HEARING

30 OCTOBER 1985

Overview of Administration Actions on Counterintelligence and Security Countermeasures

INTRODUCTION

Mr. Chairman, many of the counterintelligence (CI) and countermeasure (CM) initiatives I will discuss today have been previously outlined in recent Congressional hearings dealing with the intelligence budget and improvements in the CI and CM arenas. Others, however, will reflect some new approaches, stimulated in part by recent events, designed to strengthen our defenses against the hostile intelligence threat. All of these initiatives have resulted from the exercise of a very functional system for deriving counterintelligence and countermeasure policy, and for making legal and resource decisions. The Congress, lead by the SSCI and HPSCI, has played an important role as part of this overall system. Your interest and support of national security matters is acknowledged and appreciated. 25X1

Prior to reviewing the specifics of present and proposed administration initiatives, it is important to ensure understanding of the administration's principal organization for developing national CI and CM proposals and decisions. In January 1982, National Security Decision Directive No. 2

(NSDD-2), in part, established a number of senior interagency groups (SIGs) to assist the National Security Council (NSC) in carrying out its responsibilities. The SIG for Intelligence (SIG-I), which I chair, is the principal forum where the national perspective can be brought to CI and CM policy. The SIG-I has two subordinate interagency groups (IGs) which reflect the manner in which the Intelligence Community practices the craft of countering the foreign intelligence threat. The IG for Counterintelligence (IG/CI) is chaired by the Director of the FBI, and the IG for all other countermeasures (IG/CM) is chaired by the Deputy Undersecretary of Defense for Policy. Each agency or department of the Intelligence Community, as appropriate, is represented on these IGs, as is any other Federal Government agency or department when matters under their cognizance are being deliberated. Secretariat and staff support for these multi-agency groups is provided from elements of the DCI's Intelligence Community Staff. [redacted] 25X1

The SIG-I system supplements but does not replace other Executive Branch policy recommending and implementing entities such as the DCI Security Committee, the National Telecommunications and Information Systems Security Committee, the SIG for Technology Transfer, etc. It does, however, have the capability for and mission of ensuring proper national-level coordination of all CI and CM matters. Many national-level policy and legal issues are developed or reviewed by the IGs and referred to the SIG-I with appropriate recommendations. The SIG-I in turn endorses courses of action or refers issues to the NSC for implementation decisions. [redacted] 25X1

All Executive Branch policy recommending or policy establishing entities act upon needs identified through their own deliberations, formal studies

conducted on specific problems, or as a result of requests from Congress. One principal tool which assists in identifying needed improvements is the periodic net assessment of the "Hostile Intelligence Services Threat and US Countermeasures." This study, conducted at the direction of the NSC, defines the nature and scope of the total threat to the United States from hostile intelligence services and assesses the effectiveness of our countermeasures thereto. The recommendations resulting from these Community supported studies are subsequently acted upon by appropriate government agencies. Examples of other periodic Executive Branch formal examinations of our CI and CM posture are the 1982 study, "Capabilities Against the Hostile Intelligence Threat, 1983-1988," studies of the adequacy of US counterintelligence (March 1983) and countermeasure organizations (July 1983), CI Data Base Study (June 1983), Interagency Research and Development Council study on R&D to Counter the Foreign Intelligence Threat (September 1984), and the Macro Resources Data Study (December 1984). Each of these resulted in recommendations which have been acted upon by pertinent Federal Government agencies and departments to improve our capabilities to counter the threat. [redacted] 25X1

You will recall the actions taken to examine how best to improve our need for multidisciplinary CI analysis since this is an example of an examination specifically requested by Congress. The Community CI Staff subsequently developed its study of Multidisciplinary Analysis (November 1983) which was reviewed by the Bross Commission in arriving at its independent assessment (November 1983). As a result of this examination, we agreed on the need for more formal structuring of our deception analysis capabilities and created a National Intelligence Officer (NIO) for Foreign Denial and Intelligence Activities to provide guidance and direction to this effort. [redacted] 25X1

When circumstances indicate, ad hoc panels or committees are appointed to focus blue ribbon expertise and attention on the resolution of counter threat issues. Examples of this approach are the appointment of the Secretary of State's Advisory Panel on Overseas Security (the Inman Panel) which examined issues relating to diplomatic security in the United States and overseas, the Secretary of Defense's appointment of a commission (Stilwell Commission) to review and evaluate DOD security policies and procedures, and the Information Security Oversight Office examination of US information security policies. I will amplify the course of these efforts shortly. 25X1

The Intelligence Community structure of the SIG-I and its subordinate IGs is for policy and planning. Responsibility for CI operations rests with the FBI and CIA and the military service agencies of DOD. There is close collaboration in CI operations among the operating organizations with the DOD elements coordinating their operations with the FBI and CIA as appropriate to the locale of these operations. Security is the responsibility of the managers/commanders of the individual federal and private organizational entities. Security is complementary to CI with the Intelligence Community setting standards and policies, but implementation is the responsibility of the individual organization. 25X1

Many of you, and those of us in the Intelligence Community, have expressed concern over cases in the past year exposing agent operations by hostile intelligence services which have given them access to classified and sensitive information. The Walker case in particular has done grave damage to the national security, and there is no way to ameliorate that fact. I would

point out that US CI operations and security practices in other instances have prevented such damage. Had Thomas Cavanagh been successful in his intentions, he may well have compromised [redacted] which, in dollar value alone, 25X1 represents tens of billions of dollars. I cannot calculate the damage that would have meant to our defense posture. William Holden Bell and James Harper were exposed [redacted] Penyu 25X1 Kostadinov, a Bulgarian intelligence agent, was arrested [redacted] 25X1

[redacted] 25X1

[redacted] 25X1

[redacted] While this is gratifying, we have not let down our guard. On the 25X1 contrary, we continue to do everything within our power to look for penetrations. Working with information received from these and other defector sources, [redacted] gives, I 25X1 believe, a sound insight as to whether or not we are penetrated. [redacted] 25X1

[redacted] 25X1

The CIA has been functioning for almost 40 years. The known loss of information through espionage and defection has been remarkably low, particularly as compared with the experience of our allies in Europe. [redacted] 25X1

[redacted] 25X1

25X1

What I wish to emphasize to you is that although our defenses have occasionally been breached, the system for defending against such breaches and detecting them is alive and well and is being improved, with your help, on a continuing basis. This Committee has been apprised, in varying ways, of past accomplishments. I will review some of those results as I highlight selected initiatives now being implemented and what measures we are considering for the future in this area. Keep in mind that the SIG-I and its subordinate IGs maintain a general national context awareness of all of these initiatives which facilitates their being monitored and coordinated throughout the Federal Government.

25X1

We are and should be highly concerned about losses of information through technical penetration of all sorts -- recorders, telephones, typewriters, computers. One has to

believe, however, that media leaks which broadcast sensitive information and frequently false impressions across the world do more damage than anything else, not only to our intelligence capabilities, but also to our reputation for reliability and our ability to deal with other services and other nations. Over the last two years, 183 publications of unauthorized disclosures were reported to my Security Committee by agencies in the Intelligence Community. There were certainly more that were not reported. Among them, these agencies conducted 193 investigations of those leaks. (More than one agency may investigate the same leak.) Forty-eight cases were referred to the Department of Justice. Only one of these, the Morison case, was prosecuted. [redacted] 25X1

Virtually every kind of source we have has been damaged by unauthorized disclosures over the last couple of years. Much of it results from briefings to and gratuitous comment by Members of Congress. Talking to the press about information received in briefings jeopardizes the lives of agents. Public discussion of what we knew and when we knew it and all publication of information received in intercepted communications can result in the loss of critical sources. Statements about the Howard case indicating something very wrong at the CIA caused people around the world helping us to reconsider their cooperation. [redacted] 25X1

As I said earlier, the oversight committees are part of the problem, not all of it. [redacted] 25X1

The Executive Branch produces these damaging leaks as well as the Congress. The President has signed a directive extending the use of the polygraph in investigations involving the compromise of security information and has under consideration further steps to establish better discipline over classified information and more clear-cut workable penalties for its unauthorized use. Last year in an agreement between me and this committee, it was recognized that public references to covert action activities by either the Executive or Legislative Branches are inappropriate and that the long-established policy of the US Government is not to comment publicly on classified intelligence activities. As we stand today, you have been authorizing large sums to enhance intelligence capabilities and permitting loose talk to seriously damage their value. I am ready and anxious to take the steps necessary to correct this situation. [redacted] 25X1

WHAT'S BEING IMPLEMENTED

The IG/CI and IG/CM are currently acting on recommendations made in the 1985 national assessment of the hostile intelligence threat, the latest in a process of looking at the threat which was initiated in 1978. Fifteen recommendations were made in all. Among these are ones dealing with national policy guidance for foreign counterintelligence activities [redacted] 25X1 intelligence threat, improvement of dissemination and exchange of CI information on hostile intelligence abroad, greater SIGINT support to CI activities, a national-level policymaking body providing guidelines for counter-IMINT programs, policy changes in polygraph examinations, review of resources available for department/agency analysis, and additional interagency training in specialized areas for FCI personnel. [redacted] 25X1

STRENGTHENED FCI CAPABILITIES

CIA, the FBI and DOD are all appreciably increasing resources dedicated to CI. Since 1980, CIA has created [redacted] CI positions to be filled by 25X1 officers having CI specialities or experience and by generalist operations officers with training or experience in CI specialties. [redacted] 25X1

[redacted] 25X1

[redacted] 25X1

[redacted] 25X1

[redacted] These liaison 25X1

relationships contribute to our knowledge of the hostile services. [redacted] 25X1

We believe that the success of the CI program of CIA's Directorate of Operations is based on the premise that each and every operations officer in the Directorate, be he a covert action specialist or an operations generalist, must also be a CI officer. There are, of course, CI specialists. However, much of their job is involved in studying and analyzing the work of the operations officer who is involved in general operational work. [redacted] 25X1

We have learned [redacted] 25X1

[redacted] that the theft of Western technology is certainly high up on the 25X1

lists of requirements of the hostile services. Technology theft is also, unfortunately, a success story on their side. We are, therefore, undertaking a major program to defeat their efforts. We coordinate our efforts with many US agencies involved and often we work successfully with foreign intelligence services with whom we have a liaison relationship. [redacted] 25X1

[redacted] 25X1

Next 5 Page(s) In Document Denied

Approved For Release 2009/09/03 : CIA-RDP86M00191R000300560002-0

 25X1

[redacted]

Leaks

The unauthorized disclosure of classified information and its publication by the media continue unabated. During the past two fiscal years, 183 publications of unauthorized disclosures of classified intelligence were reported to my Security Committee by Intelligence Community agencies. Among them, these agencies conducted 193 investigations of those leaks. (More than one agency may investigate the same leak.) Forty-eight cases were referred to the Department of Justice. Only one of these, the Morison case, was prosecuted. I have already discussed some damages caused by leaks in the Achille Lauro incident. [redacted] 25X1

The disclosure of classified information to the news media by cleared individuals damages the national security. It hampers or destroys intelligence gathering operations. It helps hostile foreign governments operate against the United States. It is a reprehensible breach of trust. And it is costly to the US taxpayer. Finally, it undermines the credibility of our entire security system. The drumbeat of disclosures makes it easy for the John Walkers among us to rationalize that they are simply selling for cash that which the "official who spoke on the condition he not be named" are giving away free. [redacted] 25X1

In 40 cases, the classified information was leaked and published within 30 days of its production as an intelligence report. [redacted] 25X1

[redacted] 25X1

[redacted] Unknown does not mean the damage is not grave or serious, simply that an accurate estimate cannot be made at the time. [redacted] 25X1

There is a growing public awareness of the pernicious effect of leaks upon the national security. With Morison, we have just seen the first conviction of an individual under the Espionage Act for providing classified information to a publisher. This is good because it shows the criminal justice system can deal with aggravated cases of this type. There may be a down side, however. This conviction may be used to argue against the need for a statute to criminalize the specific crime of passing classified information to be published, thus making it available to the entire world, including the KGB. The Morison case was unique. Scores of classified leaks are published which may be just as damaging but which may never be prosecuted. We need to show the political will to stop the hemorrhaging of classified information. And there are signs that the Congress is becoming sensitized to this need. Two bills are pending which would make leaking a crime without having to call it espionage. Passage of such a law would show the will of the Congress to stop this outflow of sensitive data, would put leakers on notice that they are in greater jeopardy, and would let the public know that the government is serious about keeping its military, diplomatic, and intelligence secrets. [redacted] 25X1

Already, some segments of the media have criticized the conviction of Samuel Morison on the grounds that he was not a spy in the classic sense of working for a foreign intelligence service. The compromise of classified information, regardless of the reason, damages our security. Proposals to reduce the number of cleared people and to reduce the amount of classified information simply do not face the root of the problem. Those who are authorized to receive our secrets must behave responsibly. If everyone decides for himself which secrets will be kept and which secrets will be disclosed, we have no security. [redacted] 25X1

[redacted] there 25X1 is a reluctance to investigate leaks. Senior officials seem likely to protect their subordinates if they disclose classified information to support the boss's objectives. Most leaks come from intelligence consumers rather than its producers. Our ability to investigate, including the use of the polygraph, is weakest among those who are most likely to be the source of the leaks. [redacted] 25X1

Measures to deal with leaks are soon to be considered by the National Security Planning Group (NSPG). Options include possible proposed legislation and a system to account for and control authorized disclosures. [redacted] 25X1

Personnel Security

Personnel security is the most important part of any effective security program. No security program will be effective if, within the most elaborate

physical, technical, communications, and information security systems, there is an individual who has been cleared for access to our most vital secrets who is delivering those secrets to our opposition. While total elimination of the threat posed by such individuals may not be possible, effective measures to discourage such persons from committing treasonous acts and to expose them before extensive damage is done are under way. 25X1

The personnel security programs of US Government departments and agencies are uneven at any given time. External factors, notably resource constraints, cause variations over a period of time even in the program of a single agency. Heavy case loads and inadequate numbers of investigators and adjudicators inevitably lead to less thorough investigations and to clearance decisions which might have benefited from longer, more careful scrutiny of the investigative reports. First class personnel security programs require first line resources. 25X1

Pursuant to the statutory responsibility of the DCI to protect intelligence sources and methods, my Security Committee formulates personnel security standards for approval for access to sensitive compartmented information (SCI). These standards, embodied in Director of Central Intelligence Directive 1/14, apply universally to government employees, military personnel, contractors, and staff personnel of the legislative and judicial branches of government who receive SCI. DCID 1/14 is the only uniform and the most stringent interagency personnel security yardstick in the US Government. It authorizes polygraph testing for those employed in or affiliated with organizations which have polygraph programs. Decisions have been made in this area which I will discuss shortly. 25X1

I believe the high standards of DCID 1/14 should be applied more broadly to other sensitive information and that polygraph testing should become a mandatory procedure for all persons nominated for SCI approvals. Simple logic dictates that security processing should be the same for all of those who have access to the same information, regardless of where they are employed. We are moving to accomplish this. [redacted] 25X1

CIA is the only agency which routinely uses polygraph screening as a basic technique for all of its employees. NSA uses it for screening civilian employees and some military personnel in special access programs. Both have found empirically that the polygraph is an invaluable adjunct to personnel security investigations. [redacted] 25X1

[redacted] 25X1

CIA has placed increased emphasis on a thorough security review of new employees before they complete a three-year probationary period. This includes a full scope polygraph (both "lifestyle" and counterintelligence questions are used). Use of this program played a large role in the release from employment of Edward Lee Howard. While the policies and procedures leading to termination of Howard's CIA employment undoubtedly require close scrutiny, it is clear that polygraph testing surfaced multiple concerns about his suitability. [redacted] 25X1

A key aspect of personnel security programs is reinvestigations. People change with time. The person hired today will be significantly different,

physiologically and psychologically, ten years hence. The recognition of that dynamism is important in ensuring continued security suitability. CIA's reinvestigation program, which includes repolygraph testing, resulted [ ] terminations in FY 1984. The Scranage case resulted in part from this reinvestigation program. [ ]

25X1

25X1

We need to give more attention and study to how and why we make decisions on clearing people for access to classified information. Four decades ago, security screening for sensitive positions focused on the individual's loyalty to the United States Government. While loyalty remains important today, espionage and treason cases in recent years indicate that knowing something about the individual's own attitudes and agenda have become increasingly important. There are signs that some have enjoyed the adventure of engaging in espionage; some have spied on their country to finance lifestyles they could not have otherwise afforded; some may have turned to spying for the Soviets because they were rejected as intelligence operatives by the United States. There is little doubt that motivations for espionage are much more complex than simply embracing an alien ideology or, for that matter, simply selling out the country for money. [ ]

25X1

Our personnel security programs have been weakened to some extent by recent legal and social changes. Access to certain official records at the federal, state, and local level is being denied to non-law enforcement investigative organizations with substantive security responsibilities. Legislation may be needed to make such records available, as they once were in certain cases. [ ]

25X1

Resources are needed to build the capability to conduct a vigorous polygraph program, both for initial screening and for reinvestigations. Additional resources are also needed for R&D of new state-of-the-art polygraph instruments. [redacted] 25X1

We do exhaustive studies of recent cases of espionage against the United States and evaluate and share among Intelligence Community agencies the lessons to be learned about security and counterintelligence. Information we have gleaned from these recent cases plus that gained through the unprecedented high level of defectors provide us the opportunity to intensify such studies. [redacted] 25X1

[redacted] 25X1

25X1

[redacted] 25X1

25X1

We are moving ahead with a SECOM-sponsored project, led by USAF and FBI psychologists, to interview people convicted of espionage in an effort to improve our understanding of motivation and behavior patterns. 25X1

There is a need to expand efforts to use the behavioral sciences more effectively in initial and ongoing personnel security programs. Psychological research aimed at identifying individuals who are potential threats to security is needed, as well as studies to identify behavior which indicates a tendency to violate responsibilities for maintaining security. My Security Committee has conducted several seminars for behavioral scientists and personnel security officers, seeking to identify specific studies likely to produce useful results in this area. 25X1

Industrial Security

Industrial security is the largest of the countermeasure programs in terms of the resources involved, 25X1 during the FY 1983-FY 1985 period, and involving nearly 14,000 cleared defense facilities, over one million cleared contractor employees, and approximately 16 million classified documents entrusted to their safekeeping. 25X1

Most of the United States Government's effort in this area comes within the scope of the Defense Industrial Security Program (DISP), a comprehensive

activity administered by the Defense Investigative Service for DOD and 18 other agencies and departments. Markedly improved policy development and coordination is now effected in this area by the National Industrial Security Advisory Committee, established following a Countermeasures Organization Study recommendation. Complementing DISP efforts is the FBI's Development of Counterintelligence Awareness (DECA) program which alerts contractors in selective government projects to the danger from hostile intelligence collectors. 25X1 25X1

25X1

Next 4 Page(s) In Document Denied

Under Consideration

We have examined here what has been done in the past and what initiatives are presently being carried on. Now let us look at what the future holds. [redacted] 25X1

The espionage cases of the recent past have indicated that flaws exist in our methods of protecting sensitive US Government information from foreign collection. The presence in the United States of hostile intelligence officers has been permitted to grow to a level which has made the task of the FBI and other counterintelligence arms of the government exceedingly difficult. [redacted] 25X1

The following are some of the Presidential initiatives which are being taken to limit or prevent these breaches in our security. These steps have been worked out within the Intelligence Community, advanced through the SIG-I system to the National Security Council where they were forwarded to and approved by the President. [redacted] 25X1

[redacted] 25X1

Next 2 Page(s) In Document Denied

25X1

25X1

25X1

The use of the polygraph frequently is the only effective means of investigating unauthorized disclosures of classified information. This is a consensual crime, known only to the discloser and the recipient of the classified information. If we are to make progress toward closing off this free flow of information to unauthorized persons, increased use of the polygraph is essential.

25X1

25X1

[redacted]

Security Awareness

At Presidential direction, all agencies and departments of the US Government will embark on a new program of security awareness, with procedures established to ensure a high level of consciousness among those having access

to classified or sensitive information, to the threat from foreign sources. This program includes the requirement for periodic formal briefings on this threat. Such systems are in place in some areas. The FBI has a long-standing DECA program to alert defense industry personnel of the threat posed by hostile services. The DOD Industrial Security Program (DISP) is aimed at the Defense establishment, other federal departments and agencies, and 14,000 cleared contractor facilities with approximately 1.4 million cleared employees. Last year, a series of seminars in security awareness and education for security educators throughout the government was initiated by my Security Committee. This effort will assist in providing up-to-date information and examples for use by those responsible for security awareness programs. [redacted] 25X1

Each US Government department or agency will be required by a new Presidential initiative to establish procedures requiring employees to report contacts with all individuals of any nationality who seek sensitive or classified information, and to report any contact with nationals of criteria countries. These contacts will be reported by the responsible agency to the FBI in the case of employees in the United States, and to the CIA when the employee is located overseas. Existing reporting requirements will continue in force. [redacted] 25X1

CONCLUSION

The NSC-level SIG-I structure provides an effective mechanism for developing, monitoring, review, and coordination of counterintelligence and

other countermeasure policy and programs. We are making good progress. [redacted] 25X1

CI programs are carried out by FCI agency program managers to meet both national and departmental requirements, under NSC-level and statutory guidance. Resources are in the NFIP and managed primarily as part of the Intelligence Community budgetary process. [redacted] 25X1

Security programs are carried out by agency program managers who custom-fit and budget them to respond to the particular requirements of their department or agency's total operations. Overall security policy is set by several policymaking elements, such as the Information Security Oversight Office, DCI Security Committee, National Industrial Security Advisory Committee, among others. Interdisciplinary meshing is effected both at the NSC level and, in part, through the DCI Security Committee. Resources for security programs are largely outside of the NFIP and are not centrally managed. They are handled as part of the government's regular budgetary process involving department/agency resource managers and OMB. [redacted] 25X1

In conclusion, we are preparing to meet the increased challenges in the next few years through:

— the additional money and positions recently authorized by Congress,

— a deliberate program of building upon the unique capabilities of each organization in the Community,

— more intensive cooperation and coordination within the Intelligence Community such as you have seen on the technical security threat to our embassies,

— increasing the staff support on these issues to the DCI and DDCI with the NIO/FDIA,

— the upgrading of CI and security concerns in the State Department, and

— the new administration's policies we have discussed today and will cover further in this series of hearings.

25X1